PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN *DIGITAL SIGNATURE ALGORITHM* (DSA)

SKRIPSI

Diajukan untuk Memenuhi Sebagian dari
Syarat Memperoleh Gelar Sarjana Komputer
Program Studi Ilmu Komputer

oleh:
IRA YUSTIANA NABILA
1401493

PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN PENDIDIKAN ILMU KOMPUTER
FAKULTAS PENDIDIKAN MATEMATIKA DAN
ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA

2019

PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN *DIGITAL SIGNATURE ALGORITHM* (DSA)

Oleh

Ira Yustiana Nabila

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam

IRA YUSTIANA NABILA

1401493

PEMBANGUNAN MODEL PROTOKOL KEAMANAN PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN *DIGITAL SIGNATURE ALGORITHM* (DSA)

DISETUJUI DAN DISAHKAN OLEH PEMBIMBING:
Pembimbing I,

Rizky Rachman J.Putra, M.Kom.
NIP. 197711252006041002

Pembimbing II,

Jajang Kusnendar, M.T.
NIP. 198903252015041001

Mengetahui,
Ketua Departemen Pendidikan Ilmu Komputer,

Prof. Dr. H. Munir, M.IT
NIP. 19660325200112100

PERNYATAAN

Dengan ini saya menyatakan bahwa skripsi dengan judul "Pembangunan Model Protokol Keamanan Pada Sistem Resep Elektronik Menggunakan *Digital Signature Algorithm* (DSA)" ini sepenuhnya karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung sanksi apabila ditemukan adanya pelanggaran terhadap etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya ini.

Bandung, Januari 2019
Pembuat Pernyataan,

Ira Yustiana Nabila
NIM. 1401493

PADA SISTEM RESEP ELEKTRONIK MENGGUNAKAN *DIGITAL SIGNATURE ALGORITHM* (DSA)

Oleh

Ira Yustiana Nabila — irayustiananabila@student.upi.edu

1401493

ABSTRAK

Bidang kesehatan merupakan bidang yang sangat mungkin untuk diintegrasikan dengan adanya teknologi informasi, salah satunya pada sistem resep elektronik. Digitalisasi resep merupakan salah satu alat yang paling efektif untuk mengurangi kesalahan pengobatan serta penyalahgunaan obat tanpa resep dokter. Namun terdapat masalah yang timbul dari pengelolaan program melalui internet yaitu mengenai kerahasiaan, otentikasi keaslian tanda tangan dan integritas data dari resep elektronik. Hal tersebut dapat diatasi dengan menggunakan teknik kriptografi, salah satunya dengan menggunakan metode *digital signature algorithm* yang dikhususkan untuk tanda tangan digital. Sistem resep elektronik ini menggunakan *digital signature algorithm* untuk proses pembentukan tanda tangan dan verifikasi demi keamanan informasi, integritas data, otentikasi serta mencegah modifikasi dan akses tidak sah. Aspek kriptografi diharapkan untuk memastikan file resep pada identitas, pemeriksaan dan layanan yang diberikan benar untuk pasien atau orang yang berwenang. Dari hasil pengujian skenario *man in the middle attack* pada resep elektronik ini menunjukan bahwa 6 dari hasil pengujian resep dengan menggunakan *digital signature algorithm* dapat memberikan jaminan otentikasi pengirim dan penerima, serta dapat menjaga integritas data.

Kata Kunci: Resep Obat, Kriptografi, Tanda Tangan Digital, *Digital Signature Algorithm*.

THE DEVELOP OF A SECURITY PROTOCOL MODEL ON ELECTRONIC PRESCRIPTION SYSTEMS USING A DIGITAL SIGNATURE ALGORITHM (DSA)

Oleh

Ira Yustiana Nabila — irayustiananabila@student.upi.edu

1401493

ABSTRACT

The health sector can be very possible to be integrated with the existence of information technology. For the example, electronic prescription system. Digitalization recipes is one of the most effective tools to reduce medication errors and drug abuse without a prescription. However, there are problems that come from managing programs through the internet, there are regarding confidentiality, authentication of authenticity of signatures and integrity of data from electronic prescriptions. This matters can be solved by using cryptographic techniques, one of which is by using the digital signature algorithm method specifically for digital signatures. The electronic prescription system using a digital signature algorithm for the process of forming signatures and verification for information security, data integrity, authentication and preventing unauthorized modification and validity access. Cryptographic aspects are expected to ensure that prescription files on identity, inspection and services provided are correct for patients or authorized persons. The results of testing on electronic recipes show that the digital signature algorithm can guarantee the authenticity of senders and recipients, and can maintain data integrity. From the results of testing '*man in the middle attack'* on electronic prescriptions it proves that 6 from the test results of the prescription results using a digital signature algorithm can provide guaranteed payments and recipients, and can secure the data.

Keywords: Prescription, Cryptographi, Digital Signature, Digital Signature Algorithm.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

Amalia, D. T., & Sukohar, A. (2014). Rational drug prescription writing. *Juke Unila*, *4*(01).

Ardwiansyah, B. (2017). KEABSAHAN PENGGUNAAN TANDA TANGAN ELEKTRONIK SEBAGAI ALAT BUKTI MENURUT UNDANG--UNDANG NOMOR 11 TAHUN 2008 TENTANG INFORMASI DAN TRANSAKSI ELEKTRONIK. *LEX PRIVATUM*, *5*(7).

Arifin, S., & Dirgahayu, T. (2018). Evaluasi Implementasi Modul E-Prescribing Rumah Sakit dengan Metode Pieces. *JUITA: Jurnal Informatika*, *5*(2), 115–130.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi.

Aspden, P., Wolcott, J. A., Bootman, J. L., Cronenwett, L. R., & others. (2007). *Preventing medication errors*. National Academies Press Washington, DC.

Bell, D. S., Cretin, S., Marken, R. S., & Landman, A. B. (2004). A conceptual framework for evaluating outpatient electronic prescribing systems based on their functional capabilities. *Journal of the American Medical Informatics Association*, *11*(1), 60–70.

Cohen M. R-MS.FASHP, 1999, Medical Errors, American Pharmaceutical Association, Washington DC.

Dharma, D. (2009). Studi Perbanding Penggunaan Algoritma Hash SHA 256 dengan Simetrik dan Asimetrik Ciphers dalam Perancangan Secure SWF Rich Internet Application (RIA). Teknik Informatika, Sekolah Teknik Elektro dan Informatika.

Farida, S., Krisnamurti, D. G. B., Hakim, R. W., Dwijayanti, A., & Purwaningsih, E. H. (2018). Implementasi Peresepan Elektronik. *eJournal Kedokteran Indonesia*, 211-16.

Hahn, A., & Lovett, A. (2014). Electronic prescribing: an examination of cost effectiveness, clinician adoption and limitations. *Universal Journal of Clinical Medicine*, *2*(1), 1–24.

Handiwidjojo, W. (2015). Rekam Medis Elektronik. *Jurnal Eksplorasi Karya Sistem Informasi Dan Sains*, *2*(1).

Maryanto, B. (2008). Penggunaan Fungsi Hash Satu Arah Untuk Enkripsi Data. *Jurnal, Informatika, STMIK LIKMI, Bandung*.

Munir, R. (2006). Kriptografi. *Informatika, Bandung*.

Pajčin, B. R., & Ivaniš, P. N. (2011). Analysis of Software Realized DSA Algorithm for Digital Signature. *Guest Editorial W*, 73.

Pratiwi, A. A., & Sinuraya, R. K. (2014). Analisis Peresepan Obat Anak Usia 2--5 Tahun di Kota Bandung Tahun 2012. *Indonesian Journal of Clinical Pharmacy*, *3*(1), 18–23.

Pratiwi, P. S., & Lestari, A. (2012). E-Prescribing: Studi Kasus Perancangan dan Implementasi Sistem Resep Obat Apotik Klinik. *Speed-Sentra Penelitian Engineering Dan Edukasi*, *12*(1).

Purnama, B. E., & Winarko, E. (n.d.). Pengamanan Sistem Data Medis Menggunakan Pola Kriptografi.

Rahmawati, A., & Rahman, A. (2011). Sistem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64. *Program Studi Sistem Informasi, Universitas Ahmad Dahlan*.

Rahmawati, F., & Oetari, R. A. (2002). Kajian penulisan resep: Tinjauan aspek legalitas dan kelengkapan resep di Apotek-apotek Kotamadya Yogyakarta. *Majalah Farmasi Indonesia*, *13*(2), 86–94.

Reeves, D. (2007). The 2005 Garrod Lecture: The changing access of patients to antibiotics--for better or worse? *Journal of Antimicrobial Chemotherapy*, *59*(3), 333–341.

Salmon, J. W., & Jiang, R. (2012). E-prescribing: history, issues, and potentials. *Online Journal of Public Health Informatics*, *4*(3).

Schneier, B., & others. (1996). Applied cryptography-protocols, algorithms, and source code in C. Wiley New York.

Sligo, J., Gauld, R., Roberts, V., & Villa, L. (2017). A literature review for large-scale health information system project planning,

implementation and evaluation. *International Journal of Medical Informatics*, *97*, 86–97.

Sommerville, I. (2011). Software engineering 9th Edition. *ISBN-10*, *137035152*.

Stalling, J. (2011). *Poetics of Emptiness: Transformations of Asian Thought in American Poetry*. Oxford University Press.

Talbot, J., Welsh, D., & Welsh, D. J. A. (2006). *Complexity and cryptography: an introduction* (Vol. 13). Cambridge University Press.

Viktil, K. K., Blix, H. S., Moger, T. A., & Reikvam, A. (2007). Polypharmacy as commonly defined is an indicator of limited value in the assessment of drug-related problems. *British Journal of Clinical Pharmacology*, *63*(2), 187–195.

Wang, L., Wang, Y., Jin, S., Wu, Z., Chin, D. P., Koplan, J. P., & Wilson, M. E. (2008). Emergence and control of infectious diseases in China. *The Lancet*, *372*(9649), 1598–1605.

Winter Nick. *Scan Me: Everybody's Guide to the Magical World of QRCodes*. United States of America: Westsong. 2011.